IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent application of	Docket No.: P27325
J. L. CALVIGNAC et al.	Confirmation No.: 6208
Serial No.: 09/771,472	Group Art Unit: No. 2134
Filed: January 26, 2001	Examiner: E. C. Tran

For: **SINGLE-CYCLE HARDWARE IMPLEMENTATION OF CRYPTO FUNCTION FOR HIGH THROUGHPUT CRYPTO-PROESSING**

REQUEST FOR PRE-APPEAL BRIEF REVIEW

Commissioner for Patents
U.S. Patent and Trademark Office
Customer Window, Mail Stop AF
Randolph Building
401 Dulany Street
Alexandria, VA 22314
Sir:

This request is being filed concurrently with a Notice of Appeal and is responsive to the Final Official Action of June 13, 2006. Reconsideration and withdrawal of the 35 U.S.C. § 112, 2nd paragraph rejection and the 35 U.S.C. § 102(e) rejection is respectfully requested in view of the following remarks.

A prima facie case of indefiniteness has not been set forth and the Rejection Under 35 U.S.C. § 112, 2nd Paragraph, Is Improper

A prima facie case of anticipation has not been set forth and the Rejection Under 35 U.S.C. § 102(e) Is Improper

Examiner's Assertion

The Examiner asserts that claims 9, 11 and 17-20 are indefinite because the term "clock cycle" is indefinite because "the amount of time is not constant".

Applicant's Response

Applicant respectfully disagrees. Paragraphs [0007] and [0009] of the instant published application No. 2002/0101985 explains that the single hardware cycle may take several clock cycles or just one clock cycle. The noted claims merely recite which is disclosed in the specification. Furthermore, the Examiner has not explained how the use of the term "clock cycle" would render the claims unclear to one having ordinary skill in the art having read the specification. Applicant submits that the requirement that the claims be interpreted in light of the specification provides sufficient basis for the claims being definite. The Examiner is reminded that Applicant is entitled to the broadest reasonable interpretation permitted by the prior art, and that one of ordinary skill in the art, having read the specification, would understand what the claims define. Applicant would also like to point out that, regarding the section 112, second paragraph issues, the breadth of a claim is not to be equated with indefiniteness. Claims should not be rejected as unduly broad under 35 U.S.C. § 112, second paragraph, for non-inclusion of limitations dealing with factors which must be presumed within the level of one of ordinary skill in the art; the claims need not recite such factors where one of ordinary skill in the art to whom the specification and claims are directed would consider them obvious. *In re Skrivan*, 427 F.2d 801,166 USPQ 85 (C.C.P.A. 1970).

Examiner's Assertion

The Examiner asserts that claim 13 is indefinite because the phrase "depend solely on their inputs" is indefinite because "it fails to further limit the invention".

Applicant's Response

Applicant respectfully disagrees. Paragraph [0007] of the instant published application No. 2002/0101985 defines combinational logic as logic functions whose outputs depend solely on their inputs. The noted claims merely recite which is disclosed in the specification. Furthermore, the Examiner has not explained how the use of the noted language would render the claims unclear to one having ordinary skill in the art having read the specification.

Examiner's Assertion

The Examiner asserts that claims 1-20 are anticipated by GREENE.

Applicant's Response

Applicant respectfully disagrees. Applicant submits that a *prima facie* case of anticipation cannot be established because GREENE fails to teach each and every element of the claims.

Independent claims 1, 16 and 19 recite, *inter alia,*

> combinational logic that performs or performing computation iterations of the crypto-function on data stored in the first register and outputting data to said second register in a single hardware cycle.

GREENE does not disclose or even suggest at least this feature. While it is apparent that GREENE discloses an arrangement which utilizes an encryption circuit 102, an input buffer 104 and an output buffer 108 (see col. 5, lines 4-12) and that the encryption circuit 102 utilizes "data encryption algorithms such as DES and Triple DES, or any of various secure hash algorithms" (see col. 6, lines 58-62), GREENE does not disclose, or even suggest, combinational logic performing computation iterations of the crypto-function on data stored in the first register and outputting data to said second register in a single hardware cycle (claims 1, 16 and 19).

Examiner's Assertion

The Examiner explains that the disclosed encryption circuit 102 of GREENE is the same as the recited combinational logic performing computation iterations of the crypto-function on data stored in the first register and outputting data to said second register in a single hardware cycle.

Applicant's Response

Applicant respectfully disagrees. An encryption circuit is not the *per se* the same as combinational logic performing computation iterations of the crypto-function on data stored in the first register and outputting data to said second register in a single hardware cycle. As explained on paragraph [0005] of the instant published application No. 2002/0101985, conventional processing of crypto-functions require many clock and hardware cycles. As such processing typically occurs in an encryption circuit, the Examiner's apparent or implicit belief that all encryption circuits perform computation iterations of the crypto-function in a single hardware cycle is without prior art support.

Examiner's Assertion

The Examiner specifically points to col. 4, line 58 to col. 5, line 13 as disclosing the recited computation.

Applicant's Response

This is not correct. The noted language is entirely silent with regard to the terms "computational logic" and "crypto-function" and merely states the following:

> Various embodiments of the present invention will now be described in conjunction with a number of diagrams. The various embodiments include an encryption system that can provide higher throughput than other conventional approaches. In particular embodiments, multiple data blocks can be pipelined across one or more encryption circuits. Such an arrangement can allow a new encrypted block to be generated on each operational cycle, where a cycle can be as small as one clocked cipher stage within an encryption circuit.
> Referring now to FIG. 1, a block diagram is set forth illustrating a first embodiment. The first embodiment is designated by the general reference character 100, and is shown to include an encryption circuit 102, an input buffer/working store 104, an output buffer 108, and a scheduler 106. An encryption circuit 102 can include a number of cipher stages that enable pipelined operation. The encryption circuit 102 can process a given input data block with a latency L, where L=nT. The value n can be the number of cipher stages, and the value T is the clock period of the system, which will be no smaller than the delay introduced by the slowest cipher stage.

Examiner's Assertion

The Examiner points to col. 7, lines 7-21 and col. 7, line 62 to col. 8, line 4 as disclosing that the combinational logic performs an invertible key-dependent round function iterated a predetermined number of times (claim 5).

Applicant's Response

This is not correct. The noted language merely discloses the text identified on page 11 of the Rule 1.116 response, which is herein incorporated by reference.

Examiner's Assertion

The Examiner points to col. 7, lines 7-21 and col. 8, lines 6-32 as disclosing that the combinational logic performs mixing, permutation and key-dependent substitution in each round (claim 6).

Applicant's Response

This is not correct. The noted language merely discloses the text identified on page 12 of the Rule 1.116 response, which is incorporated by reference

Examiner's Assertion

The Examiner points to col. 7, lines 51-67 as disclosing that the combinational logic enciphers a block by performing an initial permutation of a block to be enciphered and then a complex key-dependent computation followed by a permutation which is an inverse of the initial permutation (claim 7).

Applicant's Response

This is not correct. The noted language merely discloses the text identified at the top of page 13 of the Rule 1.116 response, which is incorporated by reference.

Examiner's Assertion

The Examiner points to col. 5, lines 7-12 as disclosing that the one hardware cycle is approximately ten clock cycles (claim 9).

Applicant's Response

This is not correct. The noted language merely discloses the text identified in the middle of page 13 of the Rule 1.116 response, which is incorporated by reference

Examiner's Assertion

The Examiner points to col. 5, lines 7-12 as disclosing that the hardware implementation of the crypto-function computes an iterated round function in one clock cycle (claim 11).

Applicant's Response

This is not correct. The noted language merely discloses the text identified at the bottom of page 13 of the Rule 1.116 response, which is incorporated by reference

CONCLUSION

Reconsideration of the Final Office Action and allowance of the present application and all the claims therein are respectfully requested and now believed to be appropriate.

Should there by any questions, the Examiner is invited to contact the undersigned at the below-listed telephone number.

Respectfully submitted,
J. L. CALVIGNAC et al.

Andrew M. Calderon
Reg. No. 38,093

October 9, 2006
GREENBLUM & BERNSTEIN, P.L.C.
1950 Roland Clarke Place
Reston, VA 20191
(703) 716-1191